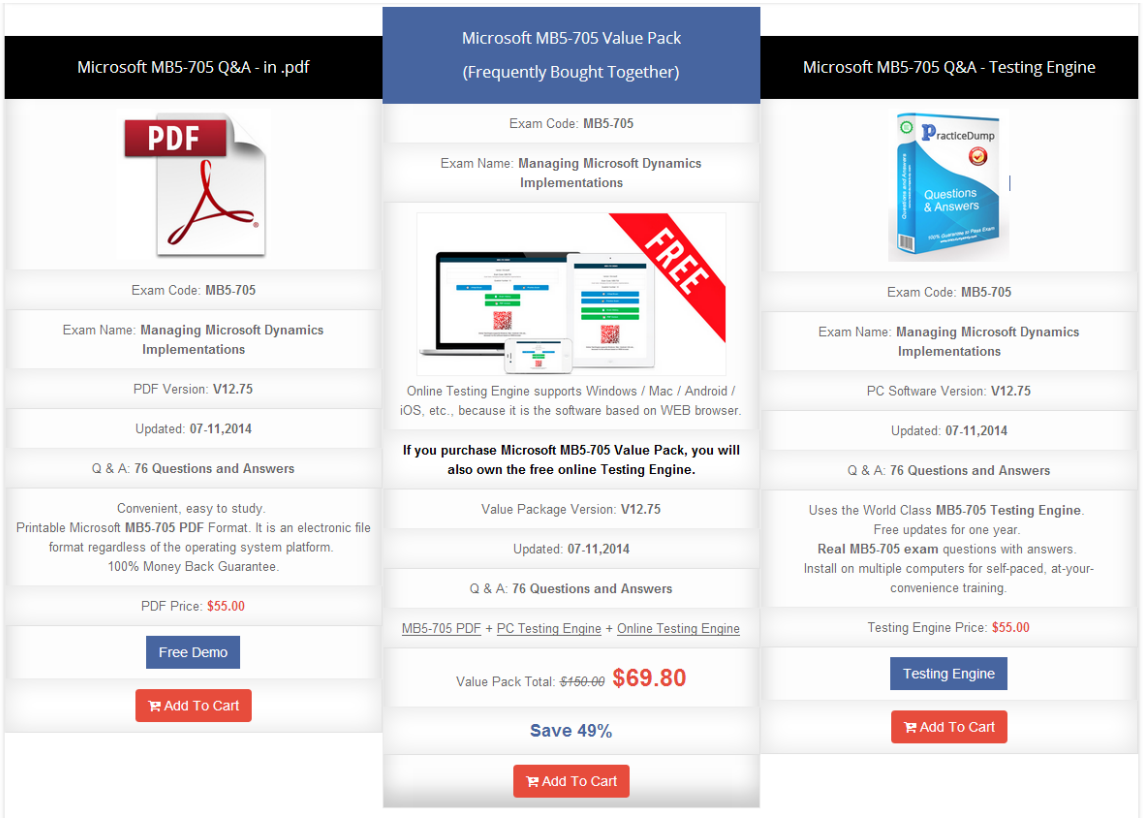
PracticeDump



http://www.practicedump.com

Free Practice Dumps - Unlimited Free Access of practice exam

Exam : **SSCP**

Title : System Security Certified Practitioner (SSCP)

Vendor : ISC

Version : DEMO

NO.1 Which of the concepts best describes Availability in relation to computer resources?
A. Users can gain access to any resource upon request (assuming they have proper permissions)
B. Users can make authorized changes to data
C. Users can be assured that the data content has not been altered
D. None of the concepts describes Availability properly
Answer: A

NO.2 _____, _____, and _____ are required to successfully complete a crime. (Choose three)
A. Root kit
B. Motive
C. Buffer Overflow
D. Means
E. Opportunity
F. Advantage
Answer: BDE

NO.3 Which of the following statements pertaining to using Kerberos without any extension is false?
A. A client can be impersonated by password-guessing.
B. Kerberos is mostly a third-party authentication protocol.
C. Kerberos uses public key cryptography.
D. Kerberos provides robust authentication.
Answer: C
Explanation:
Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network. Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:
1. Introduction
The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared session keys between clients and services and provide mutual authentication between them.
The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.
As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the client and the application service:

The Authentication Service (AS) Exchange
The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.
The Ticket Granting Service (TGS) Exchange
The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS- REP message are the request and the reply message respectively between the client and the TGS.
The Client/Server Authentication Protocol (AP) Exchange
The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys. Usually, the AS and TGS are integrated in a single device also known as the KDC.

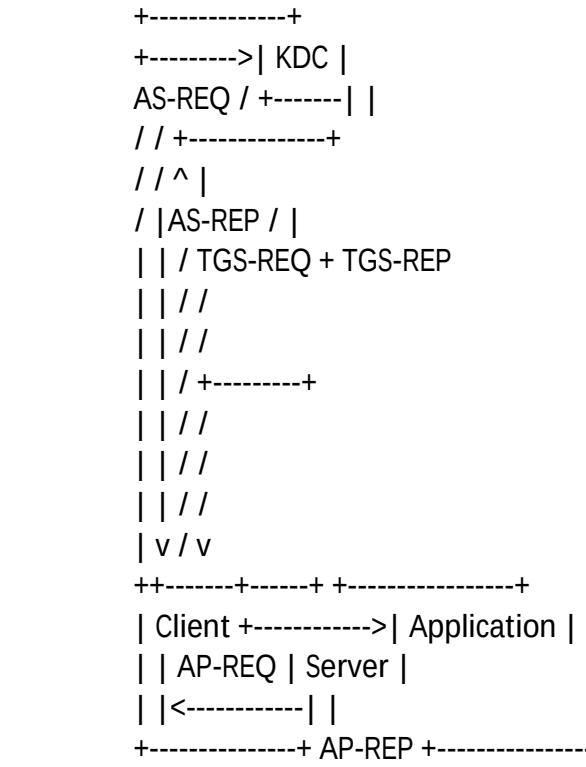


Figure 1: The Message Exchanges in the Kerberos V5 Protocol
In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key) shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.

NO.4 In a Public Key Infrastructure (PKI), what is the role of a directory server?
A. To issue certificates to users
B. To make user certificates available to others
C. Authorizes CA servers to issue certificates to users
D. Is the root authority for thePKI
Answer: B

NO.5 How often should virus definition downloads and system virus scans be completed?

A. Daily
B. Monthly
C. Weekly
D. Yearly
Answer: C

NO.6 When referring to a computer crime investigation, which of the following would be the MOST important step required in order to preserve and maintain a proper chain of custody of evidence:
A. Evidence has to be collected in accordance with all laws and all legal regulations.
B. Law enforcement officials should be contacted for advice on how and when to collect critical information.
C. Verifiable documentation indicating the who, what, when, where, and how the evidence was handled should be available.
D. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.
Answer: C
Explanation:
Two concepts that are at the heart of dealing effectively with digital/electronic evidence, or any evidence for that matter, are the chain of custody and authenticity/integrity.
The chain of custody refers to the who, what, when, where, and how the evidence was handled--from its identification through its entire life cycle, which ends with destruction or permanent archiving.
Any break in this chain can cast doubt on the integrity of the evidence and on the professionalism of those directly involved in either the investigation or the collection and handling of the evidence.
The chain of custody requires following a formal process that is well documented and forms part of a standard operating procedure that is used in all cases, no exceptions.
The following are incorrect answers:
Evidence has to be collected in accordance with all laws and legal regulations. Evidence would have to be collected in accordance with applicable laws and regulations but not necessarily with ALL laws and regulations. Only laws and regulations that applies would be followed.
Law enforcement officials should be contacted for advice on how and when to collect critical information. It seems you failed to do your homework, once you have an incident it is a bit late to do this. Proper crime investigation as well as incident response is all about being prepared ahead of time. Obviously, you are improvising if you need to call law enforcement to find out what to do.
It is a great way of contaminating your evidence by mistake if you don't have a well documented processs with clear procedures that needs to be followed.
Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation. Specific legal requirements exists for log retention and they are not the same as normal business records. Laws such as Basel, HIPPAA, SOX, and others has specific requirements.

NO.7 Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures

D. Baselines

Answer: C

Explanation:

Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks." Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards" Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions." Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.

NO.8 Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?

A. design, development, publication, coding, and testing.

B. design, evaluation, approval, publication, and implementation.

C. initiation, evaluation, development, approval, publication, implementation, and maintenance.

D. feasibility, development, approval, implementation, and integration.

Answer: C

Explanation:

The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...

NO.9 An Architecture where there are more than two execution domains or privilege levels is called:

A. Ring Architecture.

B. Ring Layering

C. Network Environment.

D. Security Models

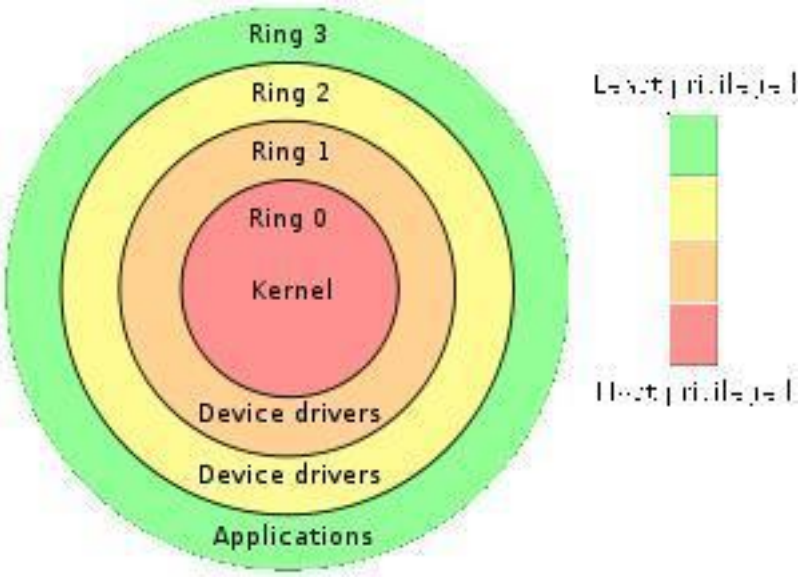
Answer: A

Explanation:

In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers.
Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
Ring Architecture



All of the other answers are incorrect because they are detractors.

NO.10 The difference between fraud and embezzlement is _____-.
A. Fraud = money or goods; embezzlement = money only
B. Fraud = removing hardware / software; embezzlement = removing data only
C. Fraud = misdemeanor; embezzlement = felony
D. There is nodifference, fraud and embezzlement are the same
E. Embezzlement is about publicity; fraud is about personal gain
Answer: A

NO.11 The Logical Link Control sub-layer is a part of which of the following?
A. The ISO/OSI Data Link layer
B. The Reference monitor
C. The Transport layer of the TCP/IP stack model
D. Change management control
Answer: A
Explanation:
The OSI/ISO Data Link layer is made up of two sub-layers; (1) the Media Access Control layer refers downward to lower layer hardware functions and (2) the Logical Link Control refers upward to higher layer software functions. Other choices are distracters.

NO.12 Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.
Answer: C
Explanation:
The Disaster Recovery Manager should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.
The following answers are incorrect:
Chief Information Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Operating Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Executive Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

NO.13 What is the Maximum Tolerable Downtime (MTD)?
A. Maximum elapsed time required to complete recovery of application data
B. Minimum elapsed time required to complete recovery of application data
C. Maximum elapsed time required to move back to primary site after a major disruption
D. It is maximum delay businesses can tolerate and still remain viable
Answer: D
Explanation:
The Maximum Tolerable Downtime (MTD) is the maximum length of time a BUSINESS FUNCTION can endure without being restored, beyond which the BUSINESS is no longer viable NIST SAYS:
The ISCP Coordinator should analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.
Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on selection of an appropriate recovery method, and the depth of detail which will be required when developing recovery procedures, including their scope and content.
Other BCP and DRP terms you must be familiar with are:
Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone

should be initiated to document the situation and plan for its mitigation.
Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD.
Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

NO.14 How would an IP spoofing attack be best classified?
A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack
Answer: A
Explanation:
IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. IP spoofing attacks is a common session hijacking attack.

NO.15 The IP header contains a protocol field. If this field contains the value of 2, what type of data is contained within the IP datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.
Answer: D
Explanation:
If the protocol field has a value of 2 then it would indicate it was IGMP.
The following answers are incorrect:
TCP. Is incorrect because the value for a TCP protocol would be 6.
UDP. Is incorrect because the value for an UDP protocol would be 17. ICMP. Is incorrect because the value for an ICMP protocol would be 1.

NO.16 When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?
A. Executive management staff
B. Senior business unit management
C. BCP committee
D. Functional business units
Answer: B
Explanation:
Many elements of a BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Executive management staff initiates the project, gives final approval and gives ongoing support. The

BCP committee directs the planning, implementation, and tests processes whereas functional business units participate in implementation and testing.

NO.17 What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

A. A capability table

B. An access control list

C. An access control matrix

D. A role-based matrix

Answer: B

Explanation:

"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188 A capability table is incorrect. "Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. The distinction that makes this an incorrect choice is that access is based on posession of a capability by the subject.

To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL." An access control matrix is incorrect. The access control matrix is a way of describing the rules for an access control strategy. The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access. CBK pp 317 - 318.

AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.

In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.

A role-based matrix is incorrect. Again, a matrix of roles vs objects could be used as a tool for thinking about the access control to be applied to a set of objects. The results of the analysis could then be implemented using RBAC.

NO.18 A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed:

A. at one end of the connection.

B. at both ends of the connection.

C. somewhere between both end points.

D. in the middle of the connection.

Answer: B

Explanation:

A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection.

In fact it would be a Multiplexer at one end and DeMultiplexer at other end or vice versa. Inverse Multiplexer at both end.

In electronics, a multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines,

which are used to select which input line to send to the output. Multiplexers are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth. A multiplexer is also called a data selector.
An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal. On the other hand, a demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the receiving end. An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch

NO.19 Insiders have a clear advantage in committing computer crime. Which two of the following do they possess? (Choose two)
A. Advantage
B. Motive
C. Outside connections
D. Means
E. Opportunity
F. Tools
Answer: DE

NO.20 At what stage of the applications development process should the security department become involved?
A. Prior to the implementation
B. Prior to systems testing
C. During unit testing
D. During requirements development
Answer: D

NO.21 Knowledge-based Intrusion Detection Systems (IDS) are more common than:
A. Network-based IDS
B. Host-based IDS
C. Behavior-based IDS
D. Application-Based IDS
Answer: C
Explanation:
Knowledge-based IDS are more common than behavior-based ID systems.
Application-Based IDS - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:

Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network-based and host-based, and knowledge-based and behavior-based:

Active and passive IDS

An active IDS (now more commonly known as an intrusion prevention system -- IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.

Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.

Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained. New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomaly-based) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they Dynamically adapt to new, unique, or original attacks. Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes.

Usage patterns that may change often and may not be static enough to implement an effective

behavior-based IDS.

NO.22 Which of the following can be used as a covert channel?
A. Storage and timing.
B. Storage and low bits.
C. Storage and permissions.
D. Storage and classification.
Answer: A
Explanation:
The Orange book requires protection against two types of covert channels, Timing and Storage.
The following answers are incorrect:
Storage and low bits. Is incorrect because, low bits would not be considered a covert channel.
Storage and permissions. Is incorrect because, permissions would not be considered a covert channel.
Storage and classification. Is incorrect because, classification would not be considered a covert channel.

NO.23 As telnet is widely know to be insecure, one time passwords (OPIE) offer a great alternative. After a user logs on remotely, OPIE will issue a challenge. What two elements will thi challenge contain?(Choose two)
A. CHAP
B. A hashed value
C. A random value
D. A seed number
E. A sequence number
Answer: DE

NO.24 Which of the following is related to physical security and is not considered a technical control?
A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks
Answer: D
Explanation:
All of the above are considered technical controls except for locks, which are physical controls.
Administrative, Technical, and Physical Security Controls
Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security

controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.
Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.
Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.

NO.25 What is NOT an authentication method within IKE and IPsec?
A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication
Answer: A
Explanation:
CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).
After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
The following were incorrect answers:
Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.
The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556

8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.
Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.
The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA).
The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.
Generally, certificate formats follow the X.509 Version 3 standard.
X.509 is part of the Open Systems Interconnect
(OSI) X.500 specification.
Public Key Authentication
Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.
In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.
Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine.
So you generate a key pair on your own computer, and you copy the public key to the server.
Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in.
Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.
There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you.
So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.

NO.26 What is also known as 10Base5?
A. Thinnet
B. Thicknet
C. ARCnet
D. UTP
Answer: B
Explanation:
Thicknet is a coaxial cable with segments of up to 500 meters, also known as 10Base5. Thinnet is a coaxial cable with segments of up to 185 meters. Unshielded twisted pair (UTP) has three variations:

10 Mbps (10BaseT), 100 Mbps (100BaseT) or 1 Gbps (1000BaseT).
ARCnet is a LAN media access method.

NO.27 The first step in the implementation of the contingency plan is to perform:
A. A firmware backup
B. A data backup
C. An operating systems software backup
D. An application software backup
Answer: B
Explanation:
A data backup is the first step in contingency planning. Without data, there is nothing to process. "No backup, no recovery".
Backup for hardware should be taken care of next.
Formal arrangements must be made for alternate processing capability in case the need should arise.
Operating systems and application software should be taken care of afterwards.

NO.28 When attempting to establish Liability, which of the following would be describe as performing the ongoing maintenance necessary to keep something in proper working order, updated, effective, or to abide by what is commonly expected in a situation?
A. Due care
B. Due concern
C. Due diligence
D. Due practice
Answer: A
Explanation:
My friend JD Murray at Techexams.net has a nice definition of both, see his explanation below:
Oh, I hate these two. It's like describing the difference between "jealously" and "envy." Kinda the same thing but not exactly. Here it goes:
Due diligence is performing reasonable examination and research before committing to a course of action. Basically, "look before you leap." In law, you would perform due diligence by researching the terms of a contract before signing it. The opposite of due diligence might be "haphazard" or "not doing your homework."
Due care is performing the ongoing maintenance necessary to keep something in proper working order, or to abide by what is commonly expected in a situation. This is especially important if the due care situation exists because of a contract, regulation, or law. The opposite of due care is "negligence."
In summary, Due Diligence is Identifying threats and risks while Due Care is Acting upon findings to mitigate risks EXAM TIP:
The Due Diligence refers to the steps taken to identify risks that exists within the environment.
This is base on best practices, standards such as ISO 27001, ISO 17799, and other consensus.
The first letter of the word Due and the word Diligence should remind you of this. The two letters are DD = Do Detect.
In the case of due care, it is the actions that you have taken (implementing, designing, enforcing, updating) to reduce the risks identified and keep them at an acceptable level. The same apply here, the first letters of the work Due and the work Care are DC. Which should remind you that DC = Do

correct.
The other answers are only detractors and not valid.

NO.29 Which method of password cracking takes the most time and effort?
A. Guessing
B. Brute Force
C. Hybrid
D. Shoulder Surfing
E. Dictionary attack
Answer: B

NO.30 What does the (star) property mean in the Bell-LaPadula model?
A. No write up
B. No read up
C. No write down
D. No read down
Answer: C
Explanation:
The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).

NO.31 What enables a workstation to boot without requiring a hard or floppy disk drive?
A. Bootstrap Protocol (BootP).
B. Reverse Address Resolution Protocol (RARP).
C. Address Resolution Protocol (ARP).
D. Classless Inter-Domain Routing (CIDR).
Answer: A
Explanation:
Bootstrap Protocol (BootP) is an Internet Layer protocol that enables a workstation to boot without requiring a hard or floppy disk drive. Reverse Address Resolution Protocol (RARP) is a TCP/IP protocol that permits a physical address, such as an Ethernet address, to be translated into an IP address. Address Resolution Protocol (ARP) is a TCP/IP protocol that permits an IP address to be translated into a physical address. Classless Inter-Domain Routing (CIDR) is a new IP addressing scheme.

NO.32 Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:
A. Peer Authentication
B. Peer Identification
C. Server Authentication
D. Name Resolution
Answer: A
Explanation:

SSL provides for Peer Authentication. Though peer authentication is possible, authentication of the client is seldom used in practice when connecting to public e-commerce web sites. Once authentication is complete, confidentiality is assured over the session by the use of symmetric encryption in the interests of better performance.
The following answers were all incorrect:
"Peer identification" is incorrect. The desired attribute is assurance of the identity of the communicating parties provided by authentication and NOT identification. Identification is only who you claim to be. Authentication is proving who you claim to be.
"Server authentication" is incorrect. While server authentication only is common practice, the protocol provides for peer authentication (i.e., authentication of both client and server). This answer was not complete.
"Name resolution" is incorrect. Name resolution is commonly provided by the Domain Name System (DNS) not SSL.

NO.33 Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?
A. Host-to-host layer
B. Internet layer
C. Network access layer
D. Session layer
Answer: B
Explanation:
The Internet layer in the TCP/IP protocol stack corresponds to the network layer (layer 3) in the OSI/ISO model. The host-to-host layer corresponds to the transport layer (layer 4) in the OSI/ISO model. The Network access layer corresponds to the data link and physical layers (layers 2 and 1) in the OSI/ISO model. The session layer is not defined in the TCP/IP protocol stack.

NO.34 An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?
A. Discretionary Access
B. Least Privilege
C. Mandatory Access
D. Separation of Duties
Answer: B

NO.35 Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?
A. Unit testing
B. Pilot testing
C. Regression testing
D. Parallel testing
Answer: C
Explanation:
Regression testing is the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original test. Unit testing refers to the testing of an

individual program or module. Pilot testing is a preliminary test that focuses only on specific and predetermined aspects of a system. Parallel testing is the process of feeding test data into two systems and comparing the results.